

CV 17-5907

**UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK**

GARAUFIS, J.

LEVY, M.J.

----- X
CAPRATE EVENTS, LLC,

Plaintiff,

Civ. No. _____

- against -

COMPLAINT

Jury Trial Demanded

ADAM KNOBLOCH,

Defendant.

----- X

Plaintiff CapRate Events, LLC ("CapRate"), by and through its attorneys, Conrad & Metlitzky LLP, alleges as follows against Defendant Adam Knobloch ("Knobloch").

NATURE OF THE ACTION

1. CapRate's former employee, Knobloch, has stolen thousands of CapRate's confidential and proprietary files, including lists containing the contact information of thousands of its customers and sponsors. In violation of the contracts he signed with CapRate, Knobloch retained the company's confidential, proprietary, and trade secret information, and since his separation from CapRate, he has exploited CapRate's stolen business assets for his own purposes and for the commercial benefit of his new employer, Bisnow, a direct competitor of CapRate's. Because informal attempts to recover CapRate's stolen data have been unsuccessful, and because Knobloch's conduct during negotiations between the parties has shown that, in the absence of judicial intervention, Knobloch intends to continue profiting from the theft of CapRate's confidential, proprietary, and trade secret information, CapRate now seeks relief from this Court. By this lawsuit, CapRate seeks to halt the theft and secure the return of its corporate assets; disgorge the ill-gotten gains that Knobloch has reaped as a result of his wrongdoing, both for

BROOKLYN OFFICE

★ OCT 10 2017 ★

IN CLERK'S OFFICE
US DISTRICT COURT E.D.N.Y.

FILED

himself and for his current employer; to recover damages for the economic losses that CapRate has suffered and will continue to suffer as a result of the ongoing misappropriation of its customers' and sponsors' trade secret information; and to recoup the substantial fees and costs that CapRate has incurred and will continue to incur in its effort to investigate and put a stop to Knobloch's illegal, willful, and malicious conduct.

2. By this Complaint, CapRate asserts the following causes of action against Knobloch: (1) violations of the Defend Trade Secrets Act, 18 U.S.C. § 1836(b); (2) misappropriation of trade secrets under New York law; (3) conversion; (4) unjust enrichment; (5) unfair competition; (6) breach of contract; and (7) violations of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030.

PARTIES

3. Plaintiff CapRate Events, LLC, is a limited liability company, organized under the laws of the State of New York, with its principal place of business in Hoboken, New Jersey.

4. Defendant Adam Knobloch is an individual who resides in Brooklyn, New York City. He is a former employee of CapRate, and his principal place of business while he was an employee of CapRate was in Queens, New York City. He is a current employee of Bisnow. On information and belief, Knobloch's principal place of business as an employee of Bisnow is Manhattan, New York City.

JURISDICTION

5. This Court has jurisdiction of this action because claims asserted by CapRate arise under the laws of the United States, specifically, the Defend Trade Secrets Act, 18 U.S.C. § 1836(c), and the Computer Fraud and Abuse Act, 18 U.S.C. § 1030. *See* 28 U.S.C. § 1331.

6. This Court has supplemental jurisdiction over the non-federal claims asserted in this action because all of the claims asserted herein by CapRate form part of the same case or controversy and arise out of a common nucleus of operative facts. *See* 28 U.S.C. § 1367(a).

7. This Court has personal jurisdiction over Knobloch because he resides in this judicial district and because a substantial part of his wrongful acts and omissions as described in this Complaint occurred within this judicial district.

VENUE

8. Venue is proper in this judicial district under 28 U.S.C. § 1391(b)(1) because Knobloch is a resident of New York and resides in this judicial district. Venue also is proper in this judicial district under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claim occurred in this judicial district.

FACTUAL ALLEGATIONS

9. The following factual allegations are common to all of the causes of action asserted by CapRate in this lawsuit.

A. CapRate Is a Digital Media and Events Company That Offers Original Content and Premiere Networking Opportunities.

10. CapRate was founded by Brian Klebash in 2011. CapRate is a digital media and events company that produces webinars and conferences.

11. CapRate's events focus on the real estate, health care, and data center industries. CapRate's events draw speakers and attendees who are industry experts and senior-level executives from established and emerging firms in these industries.

12. CapRate's events are sponsored by companies in these industries, or by companies that have services to offer to experts and executives in these industries. CapRate's sponsors are attracted to and agree to sponsor its conferences and summits because they draw a

seasoned crowd of experts and executives. In other words, CapRate's events provide a forum for corporate sponsors to gain exposure to and interact with select industry experts and executives.

13. CapRate has achieved significant commercial success since its founding and under Klebash's leadership. Based on the continuous cultivation of its network of experts and executives in its focus industries, CapRate has been able to target its audiences of seasoned industry professionals, with respect to both the persons who attend and those who speak at its events. CapRate has earned a reputation for the valuable content of its industry conferences, for the worthwhile professional networking opportunities it offers to attendees, speakers, and sponsors, and for the first-class seminars and professional development programs that are offered at its professional summits.

B. CapRate Maintains Confidential Databases and Documents with Customer and Sponsor Information That Provide CapRate With a Competitive Edge.

14. From its inception to the present, CapRate has maintained detailed records regarding the individuals who attend, participate in, speak at, or sponsor its events. These records are maintained in a variety of formats, and in a variety of files, databases, and registries. These records include detailed information about tens of thousands of customers and sponsors that have had business relationships with CapRate and who have either purchased tickets to attend or who have sponsored CapRate events in the past.

15. Much of the value of CapRate's business is derived from the detailed records it keeps regarding the customers, speakers, and sponsors who have participated in its events—or even individuals who have only expressed interest in attending or receiving information about its events. CapRate has devoted and continues to devote significant amounts of time, money, and resources to creating, developing and maintaining the confidential, nonpublic, proprietary information contained in these files and databases.

16. The files and databases that CapRate maintains regarding its customers, speakers, and sponsors includes their names, personal cell phone numbers, business phone numbers, personal email addresses, business email addresses, mailing addresses, and other contact information. Much of this contact information is not publicly available. These files and databases also include nonpublic information regarding the individual customer's, speaker's, or sponsor's historical interactions with CapRate, including the events that the individual attended or expressed interest in attending; the number and value of tickets or sponsorships purchased by the individual or the individual's employer; information about the individual's preferences regarding attendance or sponsorship of CapRate events; as well as details relating to personal interactions that CapRate has had with individual customers and sponsors, such as competitive information about the likelihood that the customers or sponsors would attend or sponsor future CapRate or similar industry events in the future.

17. While some of the information contained within these files and databases is publicly available (for example, the business contact information of certain customers or sponsors), the compilation of the data that CapRate maintains is not publicly available, nor are most of the details contained within these files and databases. It is precisely through the extensive and painstaking collection and compilation of this data that CapRate has created commercial value in the customer and sponsor information that it keeps. Indeed, the compilation or compendium of contact information and other commercially valuable data that is used by CapRate reflects a years-long process of culling and collecting the particular contacts who have directly expressed interest in, or who have demonstrated a pattern of, attending the types of industry-related events that CapRate produces.

18. For obvious reasons, CapRate's confidential compendia and collections of customer and sponsor information are valuable competitive tools. The confidential, proprietary and trade secret information contained in these files and databases provides CapRate with a competitive edge over competitors, by enabling it to produce and then market its events to a specific audience that will be interested in the content of the programs and events it hosts. The information in CapRate's files and records is extremely valuable and would benefit any individual or company that competes with CapRate, especially competitors that produce rival professional events focused on similar subject matters and target industries.

19. The information contained within CapRate's files and databases is proprietary and is not generally known to, nor readily ascertainable through proper means by, its competitors, such as Bisnow, who could profit and otherwise obtain economic value from the disclosure or use of the information. Furthermore, CapRate protects the confidentiality of its confidential, proprietary and trade secret information by storing this information in databases and computer systems that are password-protected and that can only be accessed by employees who need the information to conduct business on behalf of CapRate within the scope of their employment. The protective measures used by CapRate to safeguard its confidential, proprietary, and trade secret information include storing the company's data in cloud-based file-storage accounts through premiere hosting companies such as Microsoft or Dropbox, which provide reasonable security measures to ensure the safety of information and data stored on these platforms. Furthermore, CapRate employees who are granted access to these repositories of information must sign agreements acknowledging the confidentiality and proprietary nature of the files and databases to which they are given access, and under these agreements, CapRate's employees must acknowledge and agree that they are not to use the information outside of their roles as CapRate

employees or for the benefit of any person or entity other than CapRate. Finally, CapRate employees must agree to delete or destroy any confidential CapRate information in their possession prior to or at the termination of their employment from CapRate.

C. CapRate's Former Employee Knobloch Has a History of Misappropriating Confidential, Proprietary, and/or Trade Secret Information.

20. In June 2012, CapRate hired Knobloch into the position of Director of Business Development. As part of his role as Director of Business Development, Knobloch was required to maintain relationships with CapRate customers, sponsors, and speakers and to help CapRate expand its customer and sponsor base.

21. In the Fall of 2012, shortly after Knobloch began his employment at CapRate, CapRate was approached by one of Knobloch's previous employers, who informed CapRate that Knobloch had taken, without the company's consent, the former employer's customer list, which that company indicated contained confidential, proprietary, and trade secret information related to the former employer's business. Knobloch retained this former employer's customer list without CapRate's knowledge or approval.

22. After it learned that Knobloch had stolen his prior employer's files and customer information, CapRate took steps to make sure that Knobloch understood his obligations with respect to the protection of CapRate's own confidential, proprietary, and trade secret information, including but not limited to its customer lists and sponsor lists. To this end, CapRate required Knobloch to sign a written agreement expressly acknowledging that CapRate's customer and sponsor information was confidential, proprietary, and a trade secret. A true and correct copy of this Proprietary Information Agreement is attached to hereto as Exhibit A.

23. Knobloch therefore had actual knowledge, starting in 2012 and at all times thereafter, that CapRate considered its customer lists and sponsor lists, and all contact

information compiled therein, to be confidential, proprietary, and trade secret information.

Moreover, as he swore in the affidavit he signed in 2012, Knobloch knew that CapRate strictly forbids the theft, unauthorized retention, or unauthorized disclosure or use of its customers' and sponsors' information. Knobloch has also known, since 2012 and continuing until the present, that CapRate considers the disclosure of its confidential, proprietary, and trade secret data to third parties, or the use of that information for the benefit of third parties, especially direct competitors, as harmful to its commercial interests and a violation of CapRate's employees' contractual and other legal obligations to the company.

D. As a Condition of His Employment with CapRate, Knobloch Signed Contractual Agreements To Protect CapRate's Customer Lists, Sponsor Lists, and Other Confidential and Proprietary Information.

24. Throughout his employment at CapRate, Knobloch was given access to CapRate's proprietary, confidential, and trade secret information, as this information was necessary for him to carry out his responsibilities as CapRate's Director of Business Development. CapRate expressly informed Knobloch that the details and contact information of its customers and sponsors were confidential, proprietary, and trade secret information.

25. As discussed above, in 2012, around the start of his employment with CapRate, Knobloch signed a Proprietary Information Agreement in which he promised to protect and not to disclose CapRate's proprietary, confidential, or trade secret information. In this agreement, dated September 11, 2012, Knobloch confirmed that he understood "that CAPRATE Events, LLC's database is proprietary and protected by measures and laws." Knobloch agreed to "refrain from using" this "proprietary information" and further acknowledged that he understood "the use of information that is truly unique to firms may violate basic measures and laws concerning proprietary information and unfair competition."

26. Thereafter, as CapRate grew and evolved as a company, it took additional steps to make sure that its employees had only secure access to the customer and sponsor information that they required to perform their job duties. On June 23, 2016, only months before his departure, Knobloch signed a different Cloud Computing Policy for CapRate Events, LLC (the “Cloud Computing Policy”), in which Knobloch again promised not to take, disclose, or use confidential and proprietary CapRate information, including but not limited to any such information stored on the company’s Dropbox file-sharing account. A true and correct copy of the Cloud Computing Policy that Knobloch signed is attached hereto as Exhibit B.

27. In the Cloud Computing Policy, Knobloch acknowledged and agreed that he was “under a continuing duty not to disclose, share or sell any sensitive, confidential, proprietary or financial information of the Company,” including, “without limitation, comments or information about any specific customer, client, partner, vendor, supplier or product.” He agreed that he would not “download any data, information, documents, files or communications from the Company’s Cloud Service [including Dropbox] to devices other than any device that you use on a daily basis in connection with performing your duties for or on behalf of the Company.” And he agreed that, “[u]pon . . . separation or termination from the Company for any reason,” he would “immediately cease and desist from accessing the Company’s Cloud Service and to delete all data, information, documents, files and communications and other Company related information.”

E. After Abruptly Resigning from CapRate, Knobloch Illegally and Without Authorization Accessed CapRate’s Confidential Databases and Retained CapRate’s Confidential Files.

28. Knobloch resigned from CapRate in September 2016. His last day of work at CapRate was on September 30, 2016.

29. When he tendered his resignation, Knobloch did not tell CapRate that he was going to work for one of its direct competitors. Nor did he immediately delete all of the data, information, documents, files and communications and other Company-related information in his possession, as required by the Cloud Computing Policy he signed.

30. Instead, unbeknownst to CapRate, after business hours on the day of his departure from CapRate, and continuing into the early morning hours of the day after his departure, Knobloch continued to access CapRate's secure databases and confidential information, in violation of the Cloud Computing Policy he signed. Without the company's knowledge, consent, or permission, and after he had resigned from his employment, Knobloch accessed CapRate's Dropbox account and viewed confidential, proprietary, and trade secret information, including information relating to CapRate's sponsors.

31. Furthermore, prior to his resignation from CapRate, Knobloch "linked" his personal electronic devices to the CapRate Dropbox account, meaning that he downloaded copies of some or all of the files on CapRate's confidential cloud-based file-sharing platform onto his personal computer and mobile telephone, and, on information and belief, onto other devices. Then, in the days leading up to his departure from CapRate, Knobloch downloaded thousands of additional files containing CapRate's proprietary, confidential, and trade secret information onto his personal devices. The information downloaded by Knobloch immediately prior to his departure includes repositories of the contact information of CapRate's customers and sponsors and other valuable data regarding the operation of CapRate's business.

32. Also during this time, Knobloch added thousands of new contacts to his professional network on the professional networking website LinkedIn. In the weeks leading up to his departure from CapRate, Knobloch added hundreds of new contacts per day to his

professional network, including many individuals whose contact information is found in CapRate's customer and/or sponsor lists.

F. After Receiving His Final Sales Commissions from CapRate, Knobloch Began To Compete with CapRate As an Employee of Bisnow, Including by Using Confidential, Proprietary, and Trade Secret Information That He Unlawfully Retained from His Employment with CapRate.

33. Knobloch received his final compensation payments from CapRate, including sales commissions he had earned during his employment with CapRate, in or around March 2017. Soon afterward, Knobloch began working for CapRate's direct competitor, Bisnow.

34. Like CapRate, Bisnow produces newsletters, a website, and corporate events. Many of Bisnow's events are focused on the same economic sectors as the programs that CapRate produces, including the real estate and data center industries. Knobloch is listed on the Bisnow website as the "Sales Contact" for Bisnow events relating to "Data Centers," one of the key industries that CapRate itself serves.

35. Bisnow's events and conferences often imitate the programming, include the same speakers, and mimic similar themes as the events that CapRate creates as original content. For example, earlier this year, on April 5, 2017, CapRate produced its "Sixth Annual Greater New York Data Center Summit." Three months later, on July 26, 2017, and following Knobloch's arrival, Bisnow held a similar "Data Center Investment Conference & Expo." Bisnow's subsequent event covered many of the same topics about Data Centers as CapRate's previous summit, including the subject matter of the keynote address, and it even used similar titles and themes for panel discussions. Bisnow invited and featured speakers from the same companies at their subsequent event as CapRate had featured at its earlier event.

36. While working for Bisnow, on information and belief, Knobloch has used data, information, documents, files and other CapRate-related information that he improperly and

unlawfully kept after the end of his employment with CapRate. Indeed, on information and belief, Knobloch retained thousands of files containing CapRate's confidential, proprietary and trade secret information on multiple personal electronic devices. On information and belief, he continued to access the devices which contained CapRate's files well into the spring of 2017, and well after the beginning of his employment at Bisnow.

37. Almost immediately upon the commencement of Knobloch's employment at Bisnow, CapRate began to receive complaints from its customers regarding aggressive sales tactics that Bisnow, and in particular Knobloch, were using to solicit CapRate's contacts. For example, CapRate was informed that a customer who had not requested information from Bisnow or otherwise had any contact with that company, nevertheless had started receiving regular email solicitations and promotions regarding Bisnow events that were specifically targeted to his industry and in his region. Other customers complained to CapRate's founder and president, Brian Klebash, that they had received aggressive sales calls from Knobloch on their personal cell phones—*i.e.* because Knobloch was using contact information that is not publicly available, but that Knobloch obtained only by virtue of his employment with CapRate. Indeed, right at the beginning of Knobloch's employment with Bisnow, Klebash himself began receiving personalized email solicitations from Bisnow.

38. Not only did Knobloch engage in conduct that prompted complaints from CapRate's customers, he also has exploited CapRate's confidential, proprietary, and trade secret information on social media platforms. As an employee of Bisnow, Knobloch has used his LinkedIn account to promote Bisnow, including by promoting and touting Bisnow events on subject matters and in industries that overlap substantially with events hosted by CapRate. In doing so, Knobloch has misappropriated CapRate's customer and/or sponsor information and

used that information to promote Bisnow's competing events directly to the very proprietary network of professionals and experts that CapRate has spent years creating and cultivating.

G. Efforts To Obtain Relief from Knobloch's Unlawful Conduct Prior to Litigation Were Unsuccessful.

39. After learning of Knobloch's theft and ongoing exploitation of its confidential, proprietary, and trade secret information, CapRate confronted Knobloch and Bisnow with many of the grievances and allegations described in this Complaint. In particular, CapRate complained about Knobloch's unauthorized access to CapRate's cloud-based file-storage systems and the ongoing and unauthorized use of its stolen property, including the contact information for its customers and/or sponsors, as well as the contractual obligations that Knobloch owes to CapRate and the circumstances under which he assumed those obligations.

40. CapRate demanded that Knobloch immediately cease using any of CapRate's customer or sponsor information including, without limitation, any further contact or solicitation of any actual or potential customers identified to Bisnow by Knobloch. CapRate also demanded an accounting of the ways in which Knobloch has used the information that he retained after the termination of his employment with CapRate. Knobloch has refused to provide any explanation about how he has used the CapRate information that he stole. Indeed, despite CapRate's requests, Knobloch has refused to stop using and exploiting CapRate's confidential, proprietary, and trade secret information; to the contrary, Knobloch has continued to exploit that information for his own benefit and for the benefit of his current employer Bisnow.

H. Knobloch's Unlawful Conduct Has Benefitted Him and Bisnow Financially and Harmed CapRate's Business Performance and Prospects.

41. CapRate has incurred and continues to incur significant costs and expenses in order to investigate and identify the scope of Knobloch's wrongdoing, including but not limited to in the form of attorneys' fees and other costs of investigation.

42. Knobloch's theft and use of CapRate's confidential, proprietary, and trade secret information, including information that had been compiled in its stolen customer and sponsor lists, has benefitted Knobloch and Bisnow. After a reasonable opportunity for further investigation or discovery, there is likely to be further evidence of the specific manner in which Knobloch and Bisnow have benefitted from the use of CapRate's information, including but not limited to new and increased sponsorships for Bisnow events by persons or entities that, prior to Knobloch's employment at Bisnow, had never sponsored Bisnow's events before; increased ticket sales to its events, including from customers whose contact information was stolen from CapRate and used to promote Bisnow events and solicit ticket sales; and increased promotional and marketing exposure to the confidential network of thousands of experts and executives that CapRate spent seven years creating and protecting from unauthorized use and disclosure.

43. Similarly, after a reasonable opportunity for further investigation or discovery, CapRate is likely to establish that it has been competitively harmed by Knobloch's theft and unauthorized use of its confidential, proprietary, and trade secret information, including in the form of lost sponsorships and declines in its own ticket sales. In addition, CapRate has suffered incalculable damage to its brand by the loss of goodwill among its key constituencies, such as the experts and executives in the industries that CapRate services.

CLAIMS FOR RELIEF

FIRST CAUSE OF ACTION

(Violation of the Defend Trade Secrets Act, 18 U.S.C. § 1836(b))

44. CapRate repeats and re-alleges each and every allegation in Paragraphs 1 through 43 of the Complaint as if fully set forth herein.

45. CapRate created, developed, used, owned, and possessed the information in its confidential electronic files and databases, which include historical, recent, current, and prospective customers and sponsors of CapRate, their contact information, and other commercially valuable information related to these customers and sponsors. The data in these confidential files enable CapRate to conduct business more effectively with its customers and sponsors, including by enabling CapRate to evaluate the likelihood that a customer or sponsor will conduct business with CapRate in the future. The information contained in CapRate's files and databases is confidential, nonpublic, proprietary, and trade secret information. Knobloch had actual knowledge at all relevant times that the information contained in CapRate's databases is confidential, nonpublic, proprietary, and trade secret information.

46. CapRate has taken and continues to take reasonable steps to keep its customer- and sponsor-related information secret by, among other things, maintaining the information on password-protected platforms; limiting access to the information to only those employees who need to know the information to perform their jobs; adopting and disseminating policies—and informing employees about those policies—addressing the commercial importance and sensitivity of its confidential, proprietary and trade secret information; and by requiring employees to sign agreements—such as the Cloud Computing Policy for CapRate Events, LLC and the Proprietary Information Agreement that Knobloch signed—to obtain written commitments from employees that this information will be protected. CapRate, through the policies and agreements such as the ones signed by Knobloch, prohibits employees from uploading or saving any of its secret information on unauthorized computers or accounts, and requires employees to delete all such protected, secret information from any computer or device used by the employee upon that employee's separation from the company.

47. The confidential, proprietary, and trade secret information in CapRate's files and databases derives independent economic value from not being generally known to and not being readily ascertainable through proper means by competitors, like Knobloch and his new employer Bisnow, who could profit or otherwise obtain economic value from the disclosure or use of the information that has been compiled and collected over the course of years. CapRate has spent significant financial and human resources to develop and maintain this information, which is of substantial commercial value.

48. CapRate's confidential, proprietary and trade secret information is not readily available to the public or to CapRate's competitors, including Bisnow. CapRate derives significant economic benefit from maintaining the secrecy of its customer, sponsor, and other company information.

49. Knobloch misappropriated CapRate's trade secrets by retaining CapRate's confidential, proprietary and trade secret information after his resignation from the company. Knobloch also misappropriated CapRate's trade secrets, and subsequently used or disclosed that information, which he acquired by improper means and without the express or implied consent of CapRate.

50. Knobloch knew or had reason to know that he acquired and/or retained the trade secret information described in this Complaint under circumstances giving rise to a duty to maintain the information's secrecy.

51. Knobloch has used CapRate's trade secret information since the commencement of his employment at Bisnow, and to the benefit of Bisnow, including by soliciting CapRate's customers and/or sponsors and promoting Bisnow events to them.

52. Knobloch's conduct constitutes a willful and malicious misappropriation of CapRate's trade secrets.

53. As a consequence of Knobloch's misconduct, CapRate has suffered and will continue to suffer damages, loss of its competitive position, and irreparable harm.

SECOND CAUSE OF ACTION

(Misappropriation of Trade Secrets)

54. CapRate repeats and re-alleges each and every allegation in Paragraphs 1 through 53 of the Complaint above as if fully set forth herein.

55. CapRate possesses, owns and develops confidential, nonpublic, proprietary and trade secret information, including the customer and sponsor information contained in the CapRate files and databases described above. The information in these files and databases includes but is not limited to the contact information of historical, recent, current, and prospective CapRate customers and sponsors, and other information related to the customers and sponsors, such as the amount of money they have paid to attend or sponsor CapRate events, that enable CapRate to communicate directly with the customers and sponsors and also evaluate the probability of conducting business with them in the future.

56. The trade secret information contained in CapRate's databases is not known outside of CapRate and is only known by employees within CapRate who need the information to do their jobs. The information taken by Knobloch includes and/or was derived from the confidential, proprietary and trade secret information on CapRate's databases.

57. CapRate has taken and continues to take significant measures to guard the secrecy of its customer and sponsor information, including by, among other things, maintaining the information on password-protected platforms; limiting access to the information to only those

employees who need to know the information to perform their jobs; adopting, disseminating, and informing employees about policies addressing the commercial importance and sensitivity of its confidential, proprietary and trade secret information; requiring employees to sign agreements—such as the Cloud Computing Policy for CapRate Events, LLC and the Proprietary Information Agreement that Knobloch signed—to obtain written commitments from employees that this information will be protected. CapRate, through its policies, such as the one signed by Knobloch, precludes employees from uploading or saving any secret information on unauthorized computers or accounts, and requires employees to delete all such protected, secret information from any computer or device used by the employee upon that employee's separation from the company.

58. The customer and sponsor information in CapRate's files and databases is of great commercial value to CapRate—indeed, it is the basis on which CapRate conducts and solicits most of its business—and would be of great commercial benefit to CapRate's competitors, such as Knobloch and his new employer Bisnow.

59. CapRate expended substantial efforts and resources to develop the customer and sponsor information contained in the files and databases described in this Complaint.

60. The information contained in these files and databases cannot be properly acquired or duplicated by others, including CapRate's competitors, such as Bisnow.

61. Knobloch retained and used CapRate's trade secrets in breach of the agreements he signed with CapRate including the Cloud Computing Policy for CapRate Events, LLC and the Proprietary Information Agreement. Knobloch had a duty not to retain, use or disclose the customer information he knew to be nonpublic, confidential, proprietary, and a trade secret.

62. Knobloch has failed to return all of CapRate's trade secrets. Knobloch continued to retain and use CapRate's trade secrets after beginning his employment with Bisnow.

63. As the direct and proximate result of Knobloch's conduct, CapRate has suffered and, if this conduct is not enjoined, will continue to suffer, irreparable injury.

64. As a direct and proximate result of Knobloch's conduct, CapRate has suffered harm in an amount to be proven at trial.

65. The damages caused to CapRate by the misappropriation of its trade secrets, such as the loss of its commercial goodwill and the benefits that Knobloch and Bisnow have reaped by the exploitation of these trade secrets, including increased exposure and advertising opportunities with a trove of customer information carefully compiled by CapRate over the course of many years, are difficult to quantify in dollars and cannot be redressed by an award of money damages.

THIRD CAUSE OF ACTION

(Conversion)

66. CapRate repeats and re-alleges each and every allegation in Paragraphs 1 through 65 of the Complaint above as if fully set forth herein.

67. CapRate has rightful ownership and possession over its databases and the customer and sponsor information therein, as well as its other business files and records.

68. Knobloch, intentionally and without authority, exercised control over the confidential, proprietary and trade secret information contained in CapRate's files and databases, as well as its other business files and records, and interfered with CapRate's exclusive ownership and use of them.

69. As a direct and proximate result of Knobloch's conduct, CapRate was dispossessed and deprived of its right to the exclusive use and possession of its confidential,

proprietary and trade secret information contained in CapRate's files and databases, as well as its other business files and records.

70. Knobloch took CapRate's confidential, proprietary, and trade secret information by malice or by reckless or willful disregard of CapRate's right to exclusive possession of its files and databases.

FOURTH CAUSE OF ACTION

(Unjust Enrichment)

71. CapRate repeats and re-alleges each and every allegation in Paragraphs 1 through 70 of the Complaint above as if fully set forth herein.

72. At all relevant times, Knobloch undertook the actions described in this Complaint, including the theft of CapRate's property and its confidential business information, to benefit himself, including in the service of his new employer Bisnow, at the expense of CapRate.

73. Knobloch received benefits or enrichments by his actions. CapRate alleges that, after a reasonable opportunity for further investigation or discovery, it will show that the benefits or enrichments that Knobloch obtained for the benefit of his new employer CapRate include revenues derived from sponsorships from CapRate's own sponsors and ticket sales made to CapRate's own customers.

74. CapRate suffered an inequity or impoverishment as a result of the benefits reaped by Knobloch and Bisnow. CapRate alleges that, after a reasonable opportunity for further investigation or discovery, it will show that the inequity or impoverishment it has suffered includes the loss of sponsorships from its sponsors and ticket sales from its customers.

75. Knobloch lacked a justification for his actions.

FIFTH CAUSE OF ACTION

(Unfair Competition)

76. CapRate repeats and re-alleges each and every allegation in Paragraphs 1 through 75 of the Complaint above as if fully set forth herein.

77. Knobloch misappropriated CapRate's labor, skills, expenditures and goodwill by taking CapRate's confidential, proprietary, and trade secret information. Knobloch also has misappropriated CapRate's labor, skills, expenditures, and goodwill by soliciting customers and sponsors for the benefit of Bisnow by using confidential information acquired by Knobloch from CapRate's company files and databases.

78. CapRate spends significant time, money and effort in developing its customer and sponsor information, as well as other confidential information relating to the operation of its business, and in maintaining the secrecy of its customers' and sponsors' contact and commercial information.

79. Knobloch misappropriated CapRate's labor, skills, expenditures and goodwill by retaining, using, and failing to return CapRate's confidential, proprietary and trade secret information.

80. Knobloch acted in bad faith and out of a dishonest purpose in misappropriating CapRate's labor, skills, expenditures and goodwill. Knobloch has continued to use the confidential, proprietary and trade secret information and solicit CapRate customers and sponsors, and to promote Bisnow's events to them.

81. As a direct and proximate result of Knobloch's misconduct and bad faith, CapRate has suffered harm.

SIXTH CAUSE OF ACTION

(Breach of Contract)

82. CapRate repeats and re-alleges each and every allegation in Paragraphs 1 through 81 of the Complaint above as if fully set forth herein.

83. The Cloud Computing Policy for CapRate Events, LLC, dated June 23, 2016, is a valid and enforceable contract between CapRate and Knobloch.

84. The Proprietary Information Agreement, dated September 13, 2012, is a valid and enforceable contract between CapRate and Knobloch.

85. CapRate abided by the terms and obligations of these contracts.

86. Knobloch breached the terms of each of these contracts by, among other things, retaining CapRate's confidential, proprietary and trade secret information, including contact and other information about its customers and sponsors, without authorization. Knobloch's retention and subsequent use of this confidential, proprietary and trade secret information was done after he resigned from his employment at CapRate and without CapRate's consent.

87. As a direct and proximate result of Knobloch's breaches of these contracts, CapRate has suffered harm.

SEVENTH CAUSE OF ACTION

(Violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, *et. seq.*)

88. CapRate repeats and re-alleges each and every allegation in Paragraphs 1 through 87 of the Complaint above as if fully set forth herein.

89. CapRate's confidential, proprietary and trade secret information is stored on, and accessible from, CapRate's computers and cloud-based accounts. The CapRate computers and cloud-based accounts on which its confidential, proprietary and trade secret information is stored

are protected computers because they are used in or affect interstate or foreign commerce or communication.

90. Access to CapRate's confidential, proprietary, and trade secret information is strictly controlled and limited by security measures, including passwords that are only provided to employees who are authorized to use the information to conduct business on behalf of CapRate and for no other purpose. Access to CapRate's confidential, proprietary, and trade secret information is prohibited by the company after an employee resigns.

91. Following his resignation, Knobloch intentionally accessed the computers storing the confidential, proprietary, and trade secret information without authorization and/or in excess of the authorization granted to him, and further, he obtained valuable commercial information from those protected computers during his post-resignation access.

92. Knobloch knowingly and with intent to defraud accessed the protected computers without authorization and/or in excess of the authorization granted to him, and by means of such conduct obtained commercially valuable confidential data.

93. Knobloch knowingly caused the transmission of information without authorization and/or in excess of the authorization granted to him, and as a result of such conduct, intentionally caused damage to CapRate, including to its protected computers or accounts.

94. As a result of Knobloch's conduct, Knobloch caused, or recklessly caused, damage and loss. CapRate's damages as a result of Knobloch's unauthorized post-departure access to its protected computers exceed \$5,000.

PRAYER FOR RELIEF

WHEREFORE, CapRate requests judgment and relief against Knobloch, as follows:

1. A preliminary and/or permanent injunction:
 - a. ordering Knobloch to immediately return to CapRate all copies of the stolen data and information, including its customer and sponsor information, in his possession, whether existing in electronic or hard copy format;
 - b. ordering Knobloch to permanently remove, delete and destroy any and all of CapRate's stolen data and information, including its customer and sponsor information, in his possession, whether existing in electronic or hard copy format; and
 - c. enjoining Knobloch from using, copying or disclosing any of CapRate's stolen data and information.
2. An award of restitution in an amount to be determined at trial.
3. An award of compensatory damages in an amount to be determined at trial.
4. An award of royalties in an amount to be determined at trial.
5. An award of exemplary damages in an amount not more than two times the amount of damages awarded hereunder.
6. An award of punitive damages in an amount to be determined at trial.
7. An award of attorneys' fees, costs, and interest.
8. Such other relief as the Court deems just and appropriate.

JURY TRIAL DEMAND

Pursuant to Federal Rule of Civil Procedure 38, CapRate demands a trial by jury of all issues and causes of action that are so triable.

Respectfully submitted,

Date: October 10, 2017

CONRAD & METLITZKY LLP

A handwritten signature in black ink, appearing to read "Mark R. Conrad", is written over a horizontal line.

Mark R. Conrad
Four Embarcadero Center, Suite 1400
San Francisco, CA 94111
Tel: (415) 343-7100
Fax: (415) 343-7101
Email: mconrad@conradmetlitzky.com

Attorneys for Plaintiff CapRate Events, LLC

Exhibit A

Adam Knobloch – Proprietary Information Agreement

I, Adam Knobloch, agree as a contractor and/or employee of CAPRATE Events, LLC to refrain from using proprietary information (whether from client, past sponsor, speaker, or anyone else for that matter) without prior approval from client, and informing CAPRATE Events, LLC of the use of such information. I will immediately destroy any such information from my files that could subject CAPRATE Events, LLC or I to potential claims.

Likewise, I understand that CAPRATE Events, LLC's database is proprietary and protected by measures and laws. I understand my responsibilities as a contractor and/or employee of the company.

The use of information that is truly unique to firms may violate basic measures and laws concerning proprietary information and unfair competition.

Adam D. Knobloch

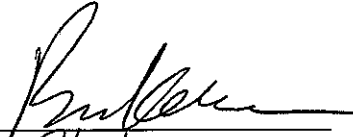


Date

9/11/2012

Countersigned:

Brian Klebash


9/13/12

Date

Exhibit B

Cloud Computing Policy for CapRate Events, LLC

This cloud computing policy applies to all employees, independent contractors and any agents of CapRate Events, LLC (the "Company") and includes all external cloud services, including without limitation cloud-based email, document storage, Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), etc. (collectively, "Cloud Services"). The Company deems this policy as necessary to protect the integrity, security and confidentiality of the Company's data, information, documents, files and communications.

- You are not permitted or authorized to open, on behalf of or for the Company, any Cloud Services account or accounts or enter into Cloud Service contracts for the storage, manipulation or exchange of Company related communications or Company owned data without the prior written consent of the Company's President, Brian Klebash.
- You are not permitted or authorized to upload to or save any of the Company's data, information, documents, files or communications to any Cloud Services account not authorized by the Company (including without limitation any personal Cloud Services account).
- Personal Cloud Services accounts may not be used for the storage, manipulation or exchange of Company related communications or the Company's data, information, documents, files and communications.
- You will be provided with access to any Company approved Cloud Services which are the only Cloud Services you are authorized to store Company related data, information, documents, files and communications.
- You are not permitted or authorized to share your login credentials for the Company's Cloud Services with anyone, including co-workers, except that you must share such information with the Company's President, Brian Klebash, who will keep a confidential document containing account information for business continuity purposes.
- You are reminded that you are under a continuing duty not to disclose, share or sell any sensitive, confidential, proprietary or financial information of the Company. This includes, without limitation, comments or information about any specific customer, client, partner, vendor, supplier or product.
- You are not authorized to share data, information, documents, files or communications stored on the Company's Cloud Service with anyone outside the Company.
- You are not authorized to download any data, information, documents, files or communications from the Company's Cloud Service to devices other than any device that you use on a daily basis in connection with performing your duties for or on behalf of the Company. In the event that any such device, including without limitation any mobile device, is lost or stolen, you agree to immediately notify the Company's President, Brian Klebash.
- Upon your separation or termination from the Company for any reason, you agree to immediately cease and desist from accessing the Company's Cloud Service and to delete all data, information, documents, files and communications and other Company related information from any device from which you have accessed the Company's Cloud Service.

ACCEPTED AND AGREED TO:

Adam Knobloch

Print Name



Signature

Director, Business Development

Title

Date: 6/23/2016